United States General Accounting Office

GAO

Testimony

Before the Committee on International Relations, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Thursday,
June 22, 2000

FOREIGN AFFAIRS

Effort to Upgrade Information Technology Overseas Faces Formidable Challenges

Statement of Jack L. Brock, Jr.
Director, Governmentwide and Defense Information Systems
Accounting and Information Management Division

G A O
Accountability * Integrity * Reliability

GAO/T-AIMD/NSIAD-00-214

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss the Department of State's efforts to improve the foreign affairs community's information technology infrastructure. As you know, the Overseas Presence Advisory Panel[1] found that many of our embassies and missions are equipped with obsolete information technology systems, which prevent efficient communication and effective information sharing and storage. In particular, many systems within our embassies are incapable of simple electronic communications across department lines and most are disparate and not interconnected. When coupled with other problems, such as poor facilities and outmoded administrative and human resource management practices, these deficiencies were found by the Panel to seriously undermine effective representation of U.S. interests abroad.

My testimony today will focus on (1) State's efforts to implement the Panel's recommendations and (2) the challenges and risks it will face as it proceeds. State has already begun providing leadership and reaching out to other federal agencies with overseas presence. At this point, State is in the early stages of planning for the common platform initiative—establishing preliminary project milestones, developing rough cost estimates, and formulating a project plan for upgrading information technology systems abroad. The detailed plan, which State intends to complete by September 30, 2000, is intended to define project goals, requirements, benefits/costs, schedule, and approval procedures.

Devising a common technology solution that will meet the collective needs of this community remains a formidable task. Over 14,000 Americans and about 30,000 foreign nationals employed by over 40 federal agencies located in 160 countries around the world comprise the foreign affairs community. Moreover, each agency has a unique mission and its own information systems and obtaining consensus may be difficult. If the common platform is to move from concept to reality, State will have to overcome cultural obstacles and get agreement on both high-level and detailed requirements of the platform's users so it can make the best decisions on the types of systems, hardware, software, and networks to acquire. Moreover, it will need to carry out this delicate balancing act while working concurrently to define its own technical architecture and continuing to address pervasive computer security weaknesses. These

[1] *America's Overseas Presence in the 21st Century: The Report of the Overseas Presence Advisory Panel,* November 1999, U.S. Department of State.

challenges must be addressed not only to minimize risk of project failure but also—and more importantly—optimize opportunities for success.

State's Efforts to Develop and Implement a Common Overseas Information Technology Platform

The Overseas Presence Advisory Panel was formed to consider the future of our nation's overseas representation, to appraise its condition, and to develop practical recommendations on how best to organize and manage our overseas posts. Last November, the Panel reported that the condition of U.S. posts and missions abroad is unacceptable. For example, the Panel found that facilities overseas are deteriorating; human resource management practices are outdated and inefficient; and there is no interagency mechanism to coordinate overseas activities or manage their size and shape.

A key finding was that our embassies and missions are equipped with antiquated, grossly inefficient, and incompatible information technology systems. According to the Panel, inefficient information systems have left the department "out of the loop," that is, other agencies, organizations, and even foreign governments are bypassing its cumbersome communications connections.

The Panel recommended that all agencies with an overseas presence provide staff with a common network featuring Internet access, e-mail, a secure unclassified Internet website, and shared applications permitting unclassified communications among all agencies and around the globe. The Panel further recommended that agencies initiate planning for a similar common platform for classified information.

In response, the President asked the Secretary of State to lead a cabinet-level committee to implement the Panel's recommendations. This is now known as the Overseas Presence Committee and is chaired by State's Undersecretary for Management. Three interagency subcommittees have been established to report to this committee, including the Rightsizing Subcommittee, the Overseas Facilities Subcommittee, and the Interagency Technology Subcommittee.

The area that you asked us to focus on, Mr. Chairman, involves the Information Technology Subcommittee, chaired by State's CIO and consisting of CIOs from the eight other major agencies with overseas presence, including the U.S. Agency for International Development, the Peace Corps, and the Departments of Defense, Justice, Transportation,

Treasury, Agriculture, and Commerce.[2] Two working groups report to this subcommittee: (1) the Interagency Technology Working Group, which is responsible for defining operational requirements, selecting specific enabling strategies, identifying required funding, and establishing standards for the common platform and (2) the Knowledge Management Working Group, which is charged with making the right information available to the right people. Knowledge management is a very important component of the Panel's recommendations. The Panel's intent is that our overseas agencies be able to not only communicate with each other and back to their respective headquarters, but also to obtain and share the information and knowledge that already exists among agencies and around the world, but is currently fragmented and not readily accessible.

State in Early Stages of Project Planning

State is in the process of developing a structured project plan for the lifecycle of its common platform initiative. In doing so, State intends to define user and system requirements; identify risks and assess technical feasibility; identify the major work elements that will be accomplished over the life of the project; analyze costs and benefits; establish project goals, performance measures, and resources; assign responsibilities; and establish milestones. It expects to complete this plan by September 30, 2000.

Given the risks, complexities, and potential costs involved in the common platform initiative, it is critical that State carefully scope the effort, anticipate and plan for risks, and establish realistic goals and milestones. Experience with similar undertakings has shown that poor project planning can cause agencies to pursue overly ambitious schedules, encounter cost overruns, and/or find themselves ill-prepared to manage risks.

To date, State has developed high-level preliminary project milestones and decided to pilot a prototype common system, from April through September 2001, at two posts, Mexico City, Mexico and New Delhi, India. It has also decided to follow a methodology for managing the project called Managing State Projects, which provides a structured process for planning, applying, and controlling funds, personnel, and physical resources to yield maximum benefits during a project life cycle. The methodology focuses on a number of key factors critical to ensuring the success of any large, complex information technology effort, including

[2]These agencies represent nearly 99 percent of our overseas presence. State and Defense together represent almost 80 percent.

(1) clearly defining what users need, (2) determining what the system will ultimately cost, and (3) defining how management will monitor and oversee progress, and ensure that the project stays on track.

State is already in the process of taking the first step—defining requirements for the overseas common technology platform. System requirements include such things as system functions, communication protocols, interfaces, regulatory requirements, security requirements, and performance characteristics. State officials responsible for managing the development of the common platform effort told us that they have developed high-level preliminary requirements and are in the process of further defining user requirements. Given the range and number of agencies and employees involved in foreign affairs, this task will need to be carefully managed. Requirements will have to be agreed upon by, and have the same meaning for, each of the participating overseas agencies, and they will need to be fully documented and sufficiently detailed so they can be used to determine what systems will be acquired and what standards will be used.

Cost estimates—the second step–cannot be finalized until user requirements are defined. As such, there is not yet firm, supported cost data on how much the new system will cost. The Panel estimated that the ultimate cost of a common solution for both classified and unclassified information will be over $300 million. The President's FY2001 budget includes $17 million in support of the recommendation for a common information technology platform for overseas offices. State officials characterized the $17 million as a "down payment" on the total anticipated investment. If these funds are appropriated, the department intends to use them on its pilot project. State is now developing preliminary cost estimates for the pilot; however, State officials told us that these estimates will be rough given that detailed user requirements have not yet been fully defined and target systems, hardware, and networks have not yet been identified.

State officials also plan to address the third step–instilling the management oversight and accountability needed to properly guide the common platform initiative. The methodology provides a formal approval process with "control gates" to ensure that user needs are satisfied by the proposed project, timetables are met, the risks are acceptable, and costs are controlled. If effectively implemented and adhered to, these control gates can provide management with the opportunity to review and formally approve progress at key decision points. State expects to define the approval process in its overall project plan.

Implementation Issues Will Prove Challenging

As State is in the early stages of project planning, it faces considerable challenges in modernizing overseas information technology systems. First, State will need to obtain agreement among its various bureaus and the agencies in the foreign affairs community on such issues as requirements, resources, responsibilities, policies, and acquisition decisions. This will be a delicate task as these agencies have different needs, levels of funding, and ongoing agency-unique systems development. Second, State needs to complete its detailed information technology architecture–or blueprint–to guide and effectively control its own information technology acquisitions. It currently has a high-level architecture and anticipates completing the detailed layers of the architecture by next year. Third, the security of the common system must be fully addressed before its deployment to ensure that sensitive data is not stolen, modified, or lost.

Barriers to Cooperation Need to Be Overcome

Obtaining the interagency cooperation and funding necessary to achieve the Panel's recommendations will be a major challenge. Each of the more than 40 agencies involved in foreign affairs has its own unique requirements, priorities, and resource constraints and many are accustomed to developing, acquiring, and maintaining their own systems. Yet State will need to overcome these cultural barriers and secure agreement on a range of issues such as which systems, hardware, and networks to acquire, how much can be spent on these assets, and who should be responsible for managing and maintaining them. In recognizing this dilemma, the Panel highlighted the need for Presidential initiative and support, the Secretary of State's leadership, and ongoing congressional oversight and support.

Addressing cultural and organizational barriers to standardization and cooperation will not be easy. First, it is likely that many agencies may want to continue operating their own technology, especially if these systems were recently acquired or upgraded. Second, no one agency by itself has the authority or ability to dictate a solution or to ensure the implementation of a mutually developed solution. Third, although negotiations are ongoing, details are still being worked out as to who will manage and administer the new collaborative network.

The department will also need to obtain cooperation among its various bureaus. Information management activities at State have historically been carried out on a decentralized basis and without the benefit of continuing centralized management attention. Consequently, systems development efforts have not always been synchronized and the systems themselves not interoperable. State acknowledges that many of its systems can be described as "stovepiped" and "islands of automation," terms which

describe their fragmentation and independence. In recognition of this problem, the department is working to establish a shared computing environment but progress has been slow.

State officials recognize that they will need to reach out to bureaus and to other agencies with overseas presence to achieve consensus on specific, detailed user requirements, acquisition decisions, standards, policies, and responsibilities and that this will be a difficult endeavor. They have told us that they have begun to explore ongoing common platform initiatives with other agencies and that they will address this challenge as they develop their overall project plan.

Lack of a Detailed Information Technology Architecture Increases Risks

Even though State is leading the common platform initiative which involves more than 40 other agencies, it does not have a detailed information technology architecture. However, State does have a high-level architecture issued last year in place and is now working to complete supporting architectural layers. An architecture is essential to guiding and constraining information technology acquisition and development efforts. In doing so, an effective architecture will limit redundancy and incompatibility among information technology systems, enable agencies to protect sensitive data and systems, and help ensure that new information technology optimally supports mission needs.

System architectures are essentially "construction plans" or blueprints that systematically detail the full breadth and depth of an organization's mission-based mode of operations in logical and technical terms. In defining architectures, agencies should systematically and thoroughly analyze and define their target operating environment—including business functions, information needs and flows across functions, and systems characteristics required to optimally support these information needs and flows. In addition, they should provide for physical and administrative controls to ensure that hardware platforms and software are not compromised.

The importance of thoroughly and systematically identifying and analyzing information needs and placing them in a technical architecture cannot be overemphasized. The Congress recognized the importance of technical architectures when it enacted the Clinger-Cohen Act, which requires chief information officers to develop, maintain, and facilitate integrated system

architectures.[3] Additionally, OMB has issued guidance[4] that, among other things, requires agency information systems investments to be consistent with federal, agency, and bureau architectures. Moreover, our reviews of other agencies have consistently shown that without a target architecture, agencies risk buying and building systems that are duplicative, incompatible, and unnecessarily costly to maintain and interface.

In April, 1999, State published a high-level information technology framework. State officials told us that documents will be produced later this year which further define the security, information applications, and technical infrastructure for the department. But, at present, State lacks the detailed framework needed to ensure that it does not build and buy systems that are duplicative, incompatible, vulnerable to security breaches, and/or are unnecessarily costly to maintain and interface. Specifically, State has not detailed its current logical and technical environment, its target environment, or specified a sequencing plan for getting from the current to the target environment. State officials told us they are working to develop these necessary architectural layers.

Such a framework is critically needed to ensure that the common platform is in concurrence with State's own target environment. If State proceeds with the common platform initiative before defining its own target architecture, it may well find that the initiative itself with its resulting decisions on standards, protocols, systems, and networks may end up driving the department's architecture. Moreover, each foreign affairs agency overseas has its own networks and systems, based on different protocols, systems, and security measures. By not having a defined and enforceable architecture, State may well perpetuate the current stovepiped, redundant, and disparate computing environment. State acknowledges that there is risk in proceeding with modernization initiatives in parallel with developing a complete information technology architecture, and it intends to begin addressing this risk as it proceeds with its pilot projects.

Computer Security Concerns Still a Challenge

As envisioned by the Panel, a common platform could provide overseas agency staff with collaborative applications and Internet access. The Panel recognized that security risks would be increased with this greater connectivity and indicated that solutions, such as the use of industry best

[3]Clinger-Cohen Act of 1996, Pub. L. No. 104-106 (40 USC 1425 (b))

[4]OMB Memorandum M-97-02, *Funding Information Systems Investments*, October 25, 1996, and OMB Memorandum M-97-16, *Information Technology Architectures*, June 18, 1997.

practices and security software, would be required to mitigate these risks. In view of these added risks, I would like to discuss specific concerns we raised in a previous review of State's computer security practices. State has generally made good progress in addressing these concerns; however, issues remain which must be paid attention to in order to ensure the integrity of the proposed platform.

Two years ago we reported[5] that the State Department's unclassified information systems and the information contained within them were vulnerable to access, change, disclosure, disruption, or even denial of service by unauthorized individuals. During penetration testing of State's systems at that time, we were able to access sensitive information and could have performed system administration actions in which we could have deleted or modified data, added new data, shut down servers, and monitored network traffic. The results of our tests showed that individuals or organizations seeking to damage State operations, commit terrorism, or obtain financial gain could possibly exploit the department's information security weaknesses. For example, by accessing State's systems, an individual could obtain sensitive information on State's administrative processes and key business processes, such as diplomatic negotiations and agreements. Our successful penetrations of State's computer resources went largely undetected during our testing, underscoring the Department's serious vulnerabilities.

Our penetration testing two years ago was successful primarily because State lacked an overall management framework and program for effectively overseeing and addressing information security risks. In particular, State lacked a central focal point for overseeing and coordinating security activities; it was not performing routine risk assessments to protect sensitive information; its information security policies were incomplete; it lacked key controls for monitoring and evaluating the effectiveness of its security programs; and it had not established a robust incident response capability. We also found that security awareness among State employees was problematic. For example, we were able to gain access to networks by guessing user passwords, bypassing physical security at one facility, and searching unattended areas for user account information and active terminal sessions.

As such, we recommended that State take a number of actions based on private sector best practices that have been shown to greatly improve

[5] *Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations* (GAO/AIMD-98-145, May 18, 1998).

organizations' ability to protect their information and computer resources. In response, State has taken a number of positive steps to address our recommendations and made real progress in strengthening its overall security program. For example, the department consolidated its previously fragmented security responsibilities and made the Chief Information Officer responsible for all aspects of the department's comprehensive computer security program; clarified in writing computer security roles and responsibilities for the Information Resources Management and Diplomatic Security offices; and enhanced its ability to detect and respond to computer security incidents by establishing a Computer Incident Response Team. In addition, the department revised its Foreign Affairs Manual to require the use of risk management by project managers and resolved the specific physical and computer security weaknesses we identified during our testing.

However, State's implementation of recommendations that are integral to successful implementation of the common platform initiative is incomplete. For example,

- State's automated intrusion detection program does not yet cover all domestic and overseas posts. As a result, State does not have a comprehensive overview of attempted or successful attacks on its worldwide systems. Lack of such a process limits State's ability to accurately detect intrusions, deal with them in a timely manner, and effectively share information about intrusions across the department.

- State lacks a mechanism for tracking and ensuring that the hundreds of recommendations made by auditors and internal vulnerability studies over the last 3 years are addressed. Again, this limits the department's ability to ensure that all relevant findings are addressed and resolved. State officials told us that action is underway to develop a tracking system.

- Lastly, even though State has formally consolidated computer security responsibilities under its CIO, its Bureau of Diplomatic Security will still be responsible for carrying out important computer security related tasks such as establishing policy, conducting security evaluations at diplomatic posts, and conducting training. As stressed in our report, fragmented responsibilities in the past have resulted in no one office being fully accountable for information technology security problems and disagreements over strategy and tactics for improvements. This new process can work, but it will be essential for the department to ensure that the Chief Information Officer effectively coordinates these responsibilities.

Consistent with our recommendations, State performed four computer security evaluations of its unclassified and sensitive but unclassified networks over the past three years. In response to your request, Mr. Chairman, we reviewed these evaluations and found that State's networks remain highly vulnerable to exploitation and unauthorized access. Because three of the four evaluation reports are classified, we are constrained in this forum from discussing specific vulnerabilities. However, each of the reports found problems indicating continuing computer security problems at the department. Collectively, the reports indicate a continuing need for the department to assess whether controls are in place and operating as intended to reduce risks to sensitive information assets. Recent media reports highlighting State problems with physical security also emphasize the need for continued vigilance in this area.

At the time of our work for this Committee, State was unable to provide much information about security features for the common platform because its design is still underway. However, based on the fact that State's networks remain vulnerable to individuals or organizations seeking to damage State operations, we emphasize the importance of effectively addressing the significant challenge that additional external connectivity brings to securing the foreign affairs community's planned information network.

Conclusions

Mr. Chairman, in summary, maintaining an effective presence overseas absolutely requires up-to-date information and communications technology. Officials overseas must have easy access to all agencies sharing the overseas platform and the fastest possible access to all information that might help them do their jobs. State is taking steps to address this need but it faces significant hurdles in doing so. Not only must it secure agreements among a wide range of disparate users and agencies, it must do so while undertaking equally challenging efforts to develop a detailed technical architecture and address continuing computer security issues. As a result, as it completes it project plan over the next few months, it is critical that State

- Carefully scope the initiative, identify and mitigate risks, analyze costs and benefits, and establish realistic goals and milestones.
- Instill the management and oversight accountability needed to properly guide the effort and secure agreement on who will manage and maintain the systems once they are implemented.

- Anticipate the steps needed to overcome cultural obstacles and employ a truly collaborative approach that can effectively facilitate agreement on requirements, priorities, resources, policies, and acquisition decisions.
- Place high priority on developing a detailed systems architecture for the department that will help ensure that information technology acquired is compatible and aligned with needs across all business areas.
- Vigorously pursue efforts to strengthen long-standing computer security weaknesses and ensure that new policies, responsibilities, and procedures being implemented are on par with best practices.

Mr. Chairman and Members of the Committee, this concludes my statement. I will be happy to answer any questions you or Members of the Committee may have.

Contacts and Acknowledgments

For questions regarding this testimony, please contact Jack L. Brock, Jr. at (202) 512-6240. Individuals making key contributions to this testimony included Cristina Chaplain, Kirk Daubenspeck, John de Ferrari, Patrick Dugan, Diana Glod, Edward Kennedy, Hai Tran, and William Wadsworth.

(511968)